



VOLUME 15, ISSUE 2

KCJIS NEWS

MAY 2013

THE KANSAS LEGISLATURE HAS PASSED TWO BILLS DIRECTLY RELATED TO KCJIS MATTERS.

ED KLUMPP

Both bills have been signed by the Governor.

House Bill 2041 section 2 amends KSA 22-4701. It provides an exception for "information regarding the release of defendants from confinement by the department of corrections or a jail" from Criminal Record History Information (CHRI). Prior to passage of this bill, the law unintentionally had included this information as CHRI making it a class A misdemeanor to publicly release the information. Of course it was never intended this information should not be released under victim notification processes. The bill was effective on April 11 when it was published in the Kansas Register.

Senate Bill 81 section 1 amends KSA 45-220, a statute in the Kansas Open Records Act. It provides open records requests for records submitted to the Central Registry and related databases must be made to the submitting agency, not the KBI or any other agency possessing the information. This was something several agencies had expressed a concern about since in most cases the Central Registry contains only the required data elements of the reports and not the complete reports in possession of the submitting agency. It also will allow the submitting agency to clarify released information or to provide additional information to a requestor. This is consistent with the philosophy that the submitting agency is the "owner" of the information. More importantly, the submitting agency is in the best position to determine if the information falls under one of the exceptions, such as information that would harm an ongoing investigation or reveal the identity of a confidential informant or undercover agent. This bill will be effective on July 1, 2013.

For more information on the 2013 legislative session go to:

www.KsLawEnforcementInfo.com/2013-session-information.html.

INSIDE THIS ISSUE:

CLOUD COMPUTING	2-4
OR NEW MANAG-	5
KCJIS-KDOR PROJECT	5-6
OR WORKING GROUP	6
2013 TRAINING SCHEDULE	7-10
WHY ARE AGENCGIES REQUIRED TO REPORT?	11-12
NAME AT TIME OF ARREST	12
JUVENILE FINGERPRINTING	13-14
AFIS TECHNOLOGY	14
HOW DOES N-DEX BENEFIT YOU?	15-16
AFIS INTERFACE	16-17
OFFENDER Q&A	17
AA REQUIREMENT EXTENDED	18-20
R.A.P.I.D	20-22
FROM THE DNA DATA-BANK	23-25
NEWS FROM THE KBI	26-
HELP DESK	32

KCJIS CONFERENCE

June 2-4, 2013

Ramada Inn, 420 SE 6th St., Topeka, KS



To Register or View Conference Schedule Go To:

KHP CJIS Launch Pad, Training -
<https://ejisaudit.khp.ks.gov/launchpad/>

Or

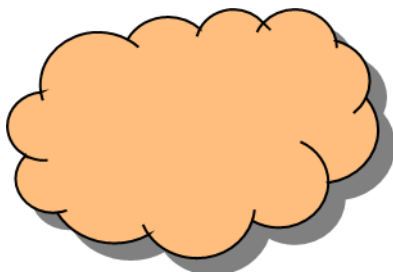
KCJIS Web Portal

If you have questions please contact Amy Johnson, KHP, at 785-296-5980 or by email at ajohnson@khp.ks.gov

CLOUD COMPUTING

Captain Randy D. Moon - Kansas Highway Patrol – CJIS Systems Officer

Reprinted from the IACP's Guiding Principles on Cloud Computing in Law Enforcement



So you think your agency is ready to make the jump to cloud computing? Not so fast! Before your agency spends a lot of time and money there are things to consider. The biggest of them from my perspective is will you be compliant with FBI & KCJIS Security Policies?

Cloud computing technologies offer substantial potential benefits to law enforcement and government agencies. Cost savings, rapid deployment of critical resources, off-site storage and disaster recovery, and dynamic provisioning of new and additional resources when needed are among the tangible benefits that cloud computing potentially offers to law enforcement agencies of all sizes. Recognizing the sensitivity of law enforcement information, and the special responsibilities that law enforcement has to ensure the accuracy, reliability, security, and availability of data within their control, however, demonstrates some of the challenges that agencies face in evaluating the potential use of this new computing paradigm.

To meet the dynamic operational needs, while maintaining the security of systems and data, law enforcement agencies using or contemplating the use of cloud computing services should ensure that their planning and implementation of cloud solutions satisfactorily address the following key principles. These principles may be embodied in contractual agreements with a cloud service provider or in service level agreements (SLAs), as appropriate.

1) FBI CJIS Security Policy Compliance – Services provided by a cloud service provider must comply with the requirements of the Criminal Justice Information Services (CJIS) Security Policy (current version 5.1, dated July 13, 2012), as it may be amended. To the extent that a law enforcement agency puts Criminal Justice Information in the cloud, the cloud provider should warrant that it has the technological and operational capabilities to meet and/or exceed the requirements of the current FBI CJIS Security Policies, and that it will make every reasonable effort to maintain compliance with these policies moving forward. The provider must acknowledge that the FBI CJIS Security Policy places restrictions and limitations on the access, use, storage, and dissemination of Criminal Justice Information and comply by those restrictions and limitations.

2) Data Ownership – Law enforcement agencies should ensure that they retain ownership of all data. Data includes all text, numerical data, database records, media files, demographic information, search history, geo-location information, meta data, or any other data and information that law enforcement users or contractors provide to a cloud service provider, or to which the cloud service provider otherwise gains access as a direct or indirect product of the cloud services provided to the law enforcement agency. The cloud provider must provide timely and appropriate notification to the law enforcement agency that owns the data of any legal process made against the cloud provider in regards to that data. No data should be released to any third party without a) proper and timely notification made to the data owner, and b) receipt of the affirmative authorization for release of said data by a duly authorized representative of the data owner, or c) receipt of an official order authorizing release of said data by a duly authorized court with jurisdiction over the data, and then only after adjudication of any legal proceedings challenging release of the data by the data owner. In all instances, the law enforcement data owner must be notified immediately of any completed unauthorized access to their data and of any unlawful or significant attempted access to their data.

Continued on Page 3

CLOUD COMPUTING - continued

3) **Impermissibility of data mining** – Law enforcement agencies should ensure that the cloud service provider does not mine or otherwise process or analyze data for any purpose not explicitly authorized by the law enforcement agency. The cloud service provider should not be permitted to data mine or otherwise process or analyze law enforcement data for purposes not explicitly authorized in the agreement with the law enforcement agency. The cloud provider should not capture, maintain, scan, index, share with third parties, or conduct any other form of data analysis or processing of law enforcement data for such purposes as advertising, product improvement, or other commercial purposes. The cloud provider may process or analyze data as necessary for ongoing and routine performance monitoring to ensure continuity of service and/or to project future dynamic provisioning requirements. The cloud provider may also process information that is made public by the law enforcement agency, either as a matter of policy or as required by law. Any agreement with a cloud service provider must take precedence over and replace any generally applicable privacy, data access or use, or similar policy of the provider which might otherwise permit data mining for purposes not explicitly authorized in the agreement.

4) **Auditing** – Upon request, or at regularly scheduled intervals mutually agreed, the cloud service provider should conduct, or allow the law enforcement agency to conduct audits of the cloud service provider's performance, use, access, and compliance with the terms of any agreement. Audits can be completed internally, by the cloud service provider under conditions and provisions mutually agreed, by outside contractors under conditions and provisions mutually agreed, or by agents of the contracting law enforcement agency at such intervals as are deemed necessary and mutually agreed.

5) **Portability and interoperability** – The cloud service provider should ensure that law enforcement data maintained by the providers is portable to other systems and interoperable with other operating systems to an extent that does not compromise the security and integrity of the data. A law enforcement agency must be able to share and/or transfer law enforcement data with other information systems and resources. Data and applications provided by a service provider should be capable of exchanging data with other

information systems and resources, and should, in-so-far as possible, be capable of exchanging data in agreed non-proprietary standards.

6) **Integrity** – The cloud service provider must maintain the physical or logical integrity of law enforcement data. The cloud service provider must maintain the integrity of law enforcement data through physical or logical separation between the cloud storage and services provided to law enforcement agencies and cloud storage and services, if any, provided to other customers. Law enforcement data may not be commingled with data in the provider's consumer cloud services, or modified in any way that compromises the integrity of the data. If the system is designed to house evidentiary material, then the cloud service provider must maintain records of access to law enforcement data sufficient to allow the law enforcement agency to establish a clear and precise chain of custody for data of evidentiary value. To the extent required by the law enforcement agency for select categories of data, the cloud provider should notify the law enforcement agency if and when it changes the physical location in which the data is stored.

7) **Survivability** – The terms of any agreement with cloud service providers should recognize potential changes in business structure, operations, and/or organization of the cloud service provider, and ensure continuity of operations and the security, confidentiality, integrity, access and utility of data. In the corporate world, mergers, acquisitions, and corporate restructuring are fairly common. Law enforcement agencies must be confident that the terms of any agreement with cloud service providers will include specific provisions to ensure continuity of operations and the continued security, confidentiality, integrity, access, and utility of all data subject to the agreement, irrespective of the commercial viability of the service provider or changes in operations, ownership, structure, technical infrastructure, and/or geographic location.



Continued on Page 4

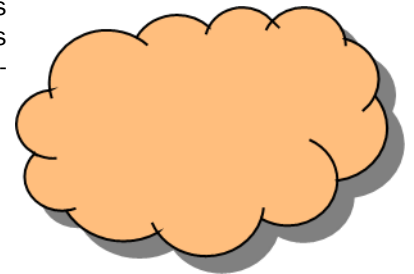
CLOUD COMPUTING - continued

8) Confidentiality – The cloud service provider should ensure the confidentiality of law enforcement data it maintains on behalf of a law enforcement agency. The provider will take all necessary physical, technical, administrative, and procedural steps to protect the confidentiality of law enforcement data. These steps may include physical security measures, access permission requirements, cyber security requirements, criminal history background security checks on employees and contractors with access to systems and data, and geographical location limitations. The confidentiality of law enforcement data may be further ensured by customer-held key encryption of the data using encryption processes. The cloud provider should provide a Certificate of Proof of Cyber security issued or approved by a duly authorized organization with appropriate credentials to verify the technical and operational capabilities and practices of the cloud provider. The cloud provider should provide timely and appropriate documentation that verifies that it currently maintains Cyber security liability insurance in an amount appropriate to the level of risk associated with managing and supporting the law enforcement agency, and agree that it will maintain said insurance throughout the course of its contracts with the law enforcement agency.

9) Availability, Reliability, and Performance – The cloud service provider must ensure that law enforcement data will be available to the law enforcement agency when it is required within agreed performance metrics. The degree to which the cloud service provider is required to ensure availability and the performance of data and services, and the reliability of its operations will be dependent on the criticality of the service provided. For some services (such as the retrieval of archived data or email), lower levels of availability and performance may be acceptable, but for more critical services, such as Computer-Aided Dispatch, reliability at a “5-nines” level (e.g. 99.999% available) may be required.

10) Cost – Law enforcement agencies should focus cloud acquisition decisions on the Total Cost of Ownership model. Cloud service purchases may use a different model for acquisition than the traditional server-based information technology solutions. Cloud services may have lower initial capital costs and permit budgetary certainty over a term of years by incorporating fixed annual operation and maintenance costs. By contrast, server system purchases typically involved larger initial capital costs and more variable annual operating and maintenance expenses. Lifetime costs of both systems will include perpetual compliance with FBI CJIS Security policies and requirements. The cost-benefit analysis of a cloud transition can only be calculated by looking at the lifetime value of the two comparable options under a Total Cost of Ownership model.

The IACP is in the process of developing model policies for cloud computing by law enforcement agencies, and these model policies are expected to be released at the International Association of Chiefs of Police Annual Conference in October 2013. In the interim, Kansas law enforcement agencies interested in implementing these principles into their current or contemplated cloud service engagements should contact the Kansas Highway Patrol to ensure that any cloud services or cloud service providers being contemplated are able to meet all FBI and KCJIS Security Policy requirements.



OFFENDER REGISTRATION'S NEW MANAGER

JESSICA DULTMEIER—KBI

While some of you may recognize my name or have attended one of my trainings, I would like to take a moment to let you know that as of April 1, 2013, I was promoted to be the next KBI Offender Registration Unit (ORU) Manager.

Just to share a little about myself; I graduated with honors from Washburn University in

May 2010 with a degree in Criminal Justice. I began working in the KBI ORU as a Senior Administrative Specialist in May 2011. In January 2012 I was promoted to the Unit's Program Consultant I position. I have participated in the Offender Registration Working Group (ORWG), attended Legislative hearings and am actively involved in the devel-

opment and deployment of KsORT (Kansas Offender Registration Tool).

At this time, there are no plans to hire another Program Consultant I, which means I will continue to provide all external Offender Registration training. I welcome the challenges this new adventure will bring and am excited for all things to come.



KCJIS-KDOR DATA INTEGRATION PROJECT

JOE MANDALA—KBI

CURRENT STATUS

The KCJIS-KDOR Data Integration Project is the effort to integrate data from the new KDOR DMV systems, both vehicle and driver, into KCJIS. Currently the vehicle interface and integration are nearly complete and some testing is being done on the driver interface. This project affects multiple systems, mainly the Central Message Switch (CMS) and the KCJIS Web Portal.

CMS INTEGRATION

CMS integration with the new DMV Vehicle system was completed last year with the implementation of "advanced searching" for vehicles. We now have more capabilities for querying DMV vehicle data than we have ever had in the past. Performance issues have been resolved, and the system has been operating very well. While some data issues at DMV remain, they are working diligently to resolve them. As always, if you have issues with vehicle queries please contact the KBI Help Desk.

Integration with the driver system on the CMS has not yet occurred. We are just now beginning to set up the new interface on our test systems so that we can begin initial and basic testing with KDOR. There is no currently known timeframe for the new DMV Driver system to go live.

KCJIS-KDOR DKCJIS-KDOR DATA INTEGRATION PROJECT—CONTINUED

KCJIS WEB PORTAL INTEGRATION

The KCJIS Web Portal integration with the new DMV Vehicle interface is nearly completed. Testing is nearly done, and a deployment plan is currently being worked out. We hope to have the new vehicle search screens available on the KCJIS Portal sometime within second quarter of this year (before July 1). The tools available on the KCJIS Portal will allow SSAP users (and others) the ability to perform the same advanced searching that Messenger users currently are able to perform on the CMS. There will also be some additional convenience and value added to the portal searches that Messenger users may wish to take advantage of. These functions and features will be detailed in documentation to the KCJIS community in the very near future.

Integration between the KCJIS Web Portal and the new DMV driver system is currently in early testing, similar to the status of the CMS Integration with the driver system. There is currently no known timeframe for the new DMV Driver system to go live.

MORE INFORMATION

More information will be made available at the KCJIS Conference in Topeka this June. There will be discussion of the new search capabilities (and limitations) on the vehicle interface for both the CMS and the Portal, and a live lab where these capabilities on the CMS can be practiced. Information about the 2013 KCJIS Conference can be found on the KCJIS Portal under Breaking News.

OFFENDER REGISTRATION WORKING GROUP

JESSICA DULTMEIER—KBI

The Offender Registration Working Group (ORWG) consists of representatives and practitioners who work daily with the offender registration system, including prosecution, department of corrections, judiciary and sheriffs' departments and provides assistance and insight to the KBI's Offender Registration Unit. Members bring input on Offender Registration policies and procedures that work as well as offer suggestions on how to improve enforcement of the Kansas Offender Registration Act. These members also serve as liaisons between the KBI Offender Registration Unit and their respective agencies. Input shared at ORWG meetings may be used when considering legislative changes. Major policy changes are referred to impacted partners prior to presentation before the Kansas Legislature.

The next ORWG meeting is scheduled for Wednesday, June 19th at 1:00, hosted by the Kansas Juvenile Correctional Complex 1430 N.W. 25th Street Topeka, Kansas 66618. If you have questions regarding the following information please contact the ORWG Chairperson Sheila Wacker at Sheila.Wacker@jocogov.org or 913-715-5470.

- Meeting dates, times and locations
- Meeting minutes (also posted on the KCJIS web portal and KBI public website)
- Copy of the agenda
- Suggestions for items to be added to the agenda
- General suggestions for the working group meetings





Kansas Bureau of Investigation

Kirk D. Thompson

Director

Derek Schmidt

Attorney General

2013 Training Schedule

The Field Support Team from the Kansas Bureau of Investigation is kicking off the 2013 Training Calendar in Topeka, Kansas. To attend the training please register with the contact listed below. When registering include the following information: specify date, class, morning or afternoon, and the names of all people from your agency will be attending. If special accommodations are needed please include a request with the registration. Please keep in mind that not all accommodations may be able to be honored. Also, please provide an email or phone number for follow-up confirmation. Register early as seating is limited!

Please register with Jancy Hunter at jancy.hunter@kbi.state.ks.us or call 785-296-7404 if you have questions.

Great Bend - Hosted by Barton County Community College

245 NE 30th Road

Great Bend, Kansas 67530

(Located two miles west of K-156; 1.5 miles east of US 281)

Tuesday - July 23rd:

<u>Room One</u>	<u>Room Two</u>	<u>Room Three</u>	<u>Time</u>
Offender Registration	10 Print Identification	Forensic Services	8:30am – noon
Criminal History Records	KIBRS	DNA	1:00pm – 4:30pm

Garden City - Hosted by the Finney County Sheriff's Office

304 N. 9th Street

Garden City, Kansas 67846

Wednesday - July 24th:

<u>Room One</u>	<u>Room Two</u>	<u>Room Three</u>	<u>Time</u>
Offender Registration	10 Print Identification	Forensic Services	8:30am – noon
Criminal History Records	KIBRS	DNA	1:00pm – 4:30pm

Continued on Page 8

2013 TRAINING SCHEDULE—CONTINUED

Oakley - Hosted by the Education Training Center

703 W. 2nd Street

Oakley, Kansas 67748

Thursday - July 25th:

<u>Room One</u>	<u>Room Two</u>	<u>Room Three</u>	<u>Time</u>
Offender Registration	10 Print Identification	Forensic Services	8:30am – noon
Criminal History Records	KIBRS	DNA	1:00pm – 4:30pm

Pittsburg – Hosted by the Memorial Auditorium

503 North Pine Street

Pittsburg, Kansas 66762

Wednesday - August 7th:

<u>Room One</u>	<u>Room Two</u>	<u>Room Three</u>	<u>Time</u>
KIBRS	DNA Databank	no afternoon class	1:00pm – 4:30pm

Thursday - August 8th:

<u>Room One</u>	<u>Room Two</u>	<u>Room Three</u>	<u>Time</u>
Criminal History Records	Offender Registration	10 Print Identification	1:00pm – 4:30pm

Concordia – Hosted by Cloud County Sheriff's Office

2090 Fort Kearney Rd

Concordia, Kansas 66901

Tuesday - September 17th:

<u>Room One</u>	<u>Room Two</u>	<u>Room Three</u>	<u>Time</u>
KIBRS	Forensic Services	DNA Databank	1:00pm – 4:30pm

Wednesday - September 18th:

<u>Room One</u>	<u>Room Two</u>	<u>Room Three</u>	<u>Time</u>
Criminal History Records	Offender Registration	10 Print Identification	1:00pm – 4:30pm

Continued on Page 9

2013 TRAINING SCHEDULE—CONTINUED

Topeka – Hosted by the Kansas Bureau of Investigation

1620 SW Tyler

Topeka, Kansas 66612

KBI Hours: 8:00am – 5:00pm. Please do not arrive prior to 8:00 am.

Tuesday – October 22nd

<u>KBI Auditorium*</u>	<u>KBI Training Room**</u>	<u>Time</u>
Offender Registration	10 Print Identification	8:30am – noon
Criminal History Records	KIBRS	1:00pm – 4:30pm

Wednesday – October 22nd

<u>KBI Auditorium</u>	<u>KBI Training Room</u>	<u>Time</u>
Criminal History Records	DNA Databank	8:30am – noon
Offender Registration	10 Print Identification	1:00pm – 4:30pm

Thursday – October 24th

<u>KBI Auditorium</u>	<u>KBI Training Room</u>	<u>Time</u>
KIBRS	DNA Databank	8:30am – noon
Forensic Services	Central Message Switch	1:00pm – 4:30pm

**** The Auditorium is located in the main building.***

*****The Training Room is located in the annex building.***

Class Synopsis

10 Print Fingerprint Identification

This instruction will include how to take and submit tenprint arrest/booking records, mug shots, and palmprints; proper use of livescan; civil fingerprinting procedures; two-finger capture devices; access to the KBI's fingerprint archive; correcting errors; and understanding AFIS reports. Practical exercises in the techniques of fingerprinting will also be included. Target Audience: anyone who takes tenprint and palmprint images for the submission of an arrest or applicant fingerprint card via livescan or hard card. This includes court personnel who fingerprint for convicted summons.

Continued on Page 10

2013 TRAINING SCHEDULE—CONTINUED

Criminal History Records

This class will cover the reporting requirements for Kansas adult and juvenile disposition reports (KADR, & KJDR). We will cover the laws and regulations governing operation, obligations of local agencies to submit records, instructions for completion of the KDR's, accessing criminal history data and the use and dissemination of criminal histories in the form of rap sheets. Target Audience: Records Clerks, Municipal and District Court clerks, law enforcement and criminal justice personnel completing fingerprint cards and/or Kansas Disposition Reports.

DNA Databank

A DNA sample can be collected from a qualifying arrestee or convicted offender in less than a minute. This single process by the booking stations or by court personnel may be the vital lead to an unsolved criminal case. This training is recommended for booking personnel, jail administrators, and court service officers. We also hope that law enforcement officers attend this class to get a better understanding of the CODIS search process, and how the DNA Databank is a vital link to your unsolved criminal cases. We will also provide an overview of the KBI's Biology Casework Section.

Forensic Services

This session will cover overall forensic services provided in the KBI's four accredited laboratories. Evidence collection, handling, submissions and discipline requirements will be addressed. A forensic scientist will be on-hand for specific discussions involving latent prints, crime scenes, and bloodstain pattern interpretation. Common concerns among law enforcement agencies as well as accreditation requirements will be included. Target Audience: All Kansas law enforcement agencies with an emphasis on detectives and crime scene personnel.

Kansas Incident Based Reporting System

The Kansas incident-based reporting system class will cover form filling of the required standard reports. Discussion of common errors as well as concerns with requirements will be included. The class will also cover recent and future changes to KIBRS, to include the new auditing program. Agencies desiring electronic submission are encouraged to attend. Target Audience: Any personnel who complete offense and arrest reports, check accuracy of those reports, and/or submit those reports to KBI.

Offender Registration

This training provides an overview of the current Kansas Offender Registration Act. The focus of training includes the duties of all registering entities and offenders. Additionally you will learn about KsORT (Kansas Offender Registration Tool), the KBI's new offender registration database and all it has to offer. NCIC training will not be provided by the KBI Offender Registration Unit. Please contact Kansas Highway Patrol in regards to NCIC matters. Target Audience: Individuals with the primary responsibility of registering offenders such as: Kansas Sheriff's Offices, County Jails, Kansas Department of Corrections, and Juvenile Justice Authority.

Central Message Switch

This training provides an overview of the tools available to users and Terminal Agency Coordinators (TACs) to access and navigate the KCJIS Central Message Switch. The focus of this training will be on KACIS, OpenFox Messenger, OpenFox Configurator, and OpenFox Archive & Retrieval. The session will begin with a one hour session to go over the basics of navigating through OpenFox Messenger, changing preferences, and locating forms and messages. The next hour will be devoted to OpenFox Archive & Retrieval, running quick searches, running detailed index searches, interpreting results, and printing reports. The last hour will be spent going over the process of adding new users into the KACIS application, reports available in KACIS and assigning message keys through Security Roles in OpenFox Configurator. Target Audience: the first two hours are for any KCJIS user who uses OpenFox. The last hour is tailored for agency TACs.

WHY ARE AGENCIES REQUIRED TO REPORT?

TINA ORTEGA - KBI

Agency Obligations to submit records to the KBI Central Repository.

K.S.A. 22-4704: requires information to be reported to the KBI Central Repository

K.S.A. 22-4705: defines what **is** a reportable event to the Central Repository. These events include, but are not limited to:

Arrests	Filing/declination of charges	Diversions
Dismissals	Acquittals	Convictions
Confinements	Appeals	

K.S.A. 21-2501: defines fingerprinting/palm print submission requirements, including the charges that are reportable to the KBI.

All Felonies

Class A and B misdemeanors

Class C assaults (defined in KSA 21-3408)

K.S.A. 38-2313: defines juvenile fingerprinting submission requirements.

All Felonies

Class A and B misdemeanors

Class C assaults (defined in KSA 21-3408)

K.S.A. 12-4517: requires the submission of fingerprints by municipal courts to the Central Repository for convictions of:

Class A or B misdemeanors

Class C assault

Violations of a municipal ordinance equivalent to the class A or B misdemeanor or class C assault

Chapter 12: Cities and Municipalities

Article 45: Code For Municipal Courts; Trials And Proceedings Incident Thereto

Statute 12-4517: Conviction of ordinances comparable to class A or B misdemeanor, assault or driving under influence of alcohol or drugs; fingerprinting; costs.

- (a) (1) The municipal court judge **shall** ensure that all persons convicted of violating municipal ordinance provisions that prohibit conduct comparable to a class A or B misdemeanor or assault as defined in **K.S.A. 21-3408** and amendments thereto under a Kansas criminal statute are fingerprinted and processed: Note: An amendment has been made per house bill 2041 and is currently in affect.

Section 1. KSA 12-4106 (e)

The municipal judge shall ensure that information concerning dispositions of city ordinance

Violations that result in convictions comparable to convictions for ~~class A and B misdemeanors~~

Offenses under Kansas criminal statutes is forwarded to the Kansas Bureau of Investigation central

Repository. This information shall be transmitted, on a form or in format approved by the Attorney

General, within 30 days of final disposition.

Continued on Page 12

WHY ARE AGENCIES REQUIRED TO REPORT?—CONTINUED

(2) The municipal court judge shall ensure that all persons arrested or charged with a violation of a city ordinance prohibiting the acts prohibited by K.S.A. 8-1567, and amendments thereto, are fingerprinted and processed at the time of booking or first appearance, whichever occurs first.

(b) The municipal court judge shall order the individual to be fingerprinted at an appropriate location as determined by the municipal court judge. Failure of the person to be fingerprinted after court order issued by the municipal judge shall constitute contempt of court. To reimburse the city or other entity for costs associated with fingerprinting, the municipal court judge may assess reasonable court costs, in addition to the court costs imposed by the state or municipality.

Amended effective July 1, 2009 due to changes in bill 2096 section 8, now requiring fingerprints on notice to appears for DUI in municipal courts at first appearance.

K.S.A 12-4412: *requires municipal courts to report diversions*

NAME USED AT TIME OF ARREST

SHERI SHARP—KBI

It is very important when you are transmitting or sending a person's demographic information on a fingerprint card that you consistently use the same information on all related documents. Booking, Arrest Reports, Offense Reports, KADR, and Court Documents need to all have the same information on them.

When an individual is booked or housed at a jail, it may be discovered that the individual is using another identity or has used another identity in the past. When fingerprinting an individual you must fingerprint them with the identity they gave at the time of the arrest. It is possible through prior contact with the individual that you know them by a different identity. Please put all the other identities, including the true identities, in the alias portion of the fingerprint card for that arrest. The Booking information, Arrest Reports, and Offense Reports will have already been generated with the identity the individual claimed upon arrest. You may want to notify the original arresting agency of the other identities so they can determine if additional charges should be filed.

If it is the first time a person is arrested and it is discovered that they use a false identity, then you can submit a correction form to request the submitted name be moved to an alias and the real name be moved to the master name. This change does not change the name of the individual at the time of the arrest. It only changes what name appears first on the list on the rapsheet. Please note that you CAN NOT change the fingerprint card and resend it electronically because the changes will not be made to the federal record. This is a manual process for the KBI. The FBI will not change their master name. The only option is to add the true information to the federal record as an AKA.



JUVENILE FINGERPRINTING REQUIREMENTS

SHERI SHARP—KBI

It has recently come to our attention that many agencies are under the impression that there is no fingerprinting requirement for juveniles or if they took fingerprints they were not to send them to the Kansas Bureau of Investigation (KBI) Central Repository. The confusion occurred due to the recodification of the juvenile statutes in the 2006 legislation year. When the new laws went into effect on January 1, 2007, K.S.A. 38-2313 did not require juveniles to be fingerprinted or photographed at the time of arrest. The mistake was realized immediately and legislation was passed by April of 2007 to require fingerprinting and photographing of juveniles. The updates went into effect upon publication.

The current statute requires that agencies take fingerprints of juveniles at the time of arrest, or first appearance or before final sentencing of any felony, or a class A or B misdemeanor or assault then send them to the KBI Central Repository.

If you are an arresting agency please communicate with the juvenile booking agency to ensure they are fingerprinting juveniles and sending the prints to the KBI central repository.

38-2313. Fingerprints and photographs. (a) Fingerprints or photographs shall not be taken of any juvenile who is taken into custody for any purpose, except that:

(1) Fingerprints or photographs of a juvenile may be taken if authorized by a judge of the district court having jurisdiction;
(2) **a juvenile's fingerprints shall be taken, and photographs of a juvenile may be taken, immediately upon taking the juvenile into custody or upon first appearance or in any event before final sentencing, before the court for an offense which, if committed by an adult, would constitute the commission of a felony, a class A or B misdemeanor or assault, as defined in subsection (a) of K.S.A. 2012 Supp. 21-5412, and amendments thereto;**

(3) fingerprints or photographs of a juvenile may be taken under K.S.A. 21-2501, and amendments thereto, if the juvenile has been: (A) Prosecuted as an adult pursuant to K.S.A. 2012 Supp. 38-2347, and amendments thereto; or (B) taken into custody for an offense described in subsection (n)(1) or (n)(2) of K.S.A. 2012 Supp. 38-2302, and amendments thereto;

(4) fingerprints or photographs shall be taken of any juvenile admitted to a juvenile correctional facility; and

(5) photographs may be taken of any juvenile placed in a juvenile detention facility. Photographs taken under this paragraph shall be used solely by the juvenile detention facility for the purposes of identification, security and protection and shall not be disseminated to any other person or agency except after an escape and necessary to assist in apprehension.

(b) Fingerprints and photographs taken under subsection (a)(1) or (a)(2) shall be kept readily distinguishable from those of persons of the age of majority. Fingerprints and photographs taken under subsections (a)(3) and (a)(4) may be kept in the same manner as those of persons of the age of majority.

(c) Fingerprints and photographs of a juvenile shall not be sent to a state or federal repository, except that:

(1) Fingerprints and photographs may be sent to the state and federal repository if authorized by a judge of the district court having jurisdiction;



Continued on Page 14

JUVENILE FINGERPRINTING REQUIREMENTS—CONTINUED

- (2) a juvenile's fingerprints shall, and photographs of a juvenile may, be sent to the state and federal repository if taken under subsection (a)(2) or (a)(4); and
- (3) fingerprints or photographs taken under subsection (a)(3) shall be processed and disseminated in the same manner as those of persons of the age of majority.
- (d) Fingerprints or photographs of a juvenile may be furnished to another juvenile justice agency, as defined by K.S.A. 2012 Supp. 38-2325, and amendments thereto, if the other agency has a legitimate need for the fingerprints or photographs.
- (e) Any fingerprints or photographs of an alleged juvenile offender taken under the provisions of subsection (a)(2) of K.S.A. 38-1611, prior to its repeal, may be sent to a state or federal repository on or before December 31, 2006.
- (f) Any law enforcement agency that willfully fails to submit any fingerprints or photographs required by this section shall be liable to the state for the payment of a civil penalty, recoverable in an action brought by the attorney general, in an amount not exceeding \$500 for each report not made. Any civil penalty recovered under this subsection shall be paid into the state general fund.
- (g) The director of the Kansas bureau of investigation shall adopt any rules and regulations necessary to implement, administer and enforce the provisions of this section, including time limits within which fingerprints shall be sent to a state or federal repository when required by this section.
- (h) Nothing in this section shall preclude the custodian of a juvenile from authorizing photographs or fingerprints of the juvenile to be used in any action under the Kansas parentage act, K.S.A. 2012 Supp. 23-2201 et seq., and amendments thereto.

History: L. 2006, ch. 169, § 13; L. 2007, ch. 23, § 1; L. 2011, ch. 30, § 163; L. 2012, ch. 162, § 68; May 31

AFIS TECHNOLOGY SUPPORTED BY THE KBI AFIS

ELY MEZA—KBI

Livescan Technology:

As part of the new AFIS implementation in 2007, the KBI adopted the current FBI fingerprint resolution standards of 1000 pixels-per-inch (ppi), and added the ability to receive palm prints and mug shots electronically via livescan, all of which dramatically increase the chance to quickly identify an individual not only with-

in Kansas but nationally. Many agencies in the state are still using older livescans however, that cannot provide fingerprints at greater than 500 ppi resolution and cannot provide palm prints or mug shots.

As you make budget plans and look for grant opportunities, please consider the adoption of newer livescans that can meet

current standards.

Agencies interested in the livescan technology or with AFIS related questions should contact Ely Meza at (785) 296-8254 or ely.meza@kbi.state.ks.us.



HOW DOES N-DEX BENEFIT ME?

AMY JOHNSON

What is N-DEX?

The National Data Exchange (N-DEX) is a repository of criminal justice records, available in a secure online environment, managed by the FBI's Criminal Justice Information Services (CJIS) Division.

N-DEX brings together data from criminal justice agencies throughout the United States, including:

- Incident and case reports
- Arrest reports
- Computer-aided dispatch calls
- Traffic citations
- Narratives
- Photos
- Supplements
- Booking and incarceration data
- Parole/probation information

N-DEX automatically correlates and resolves data from open and closed reports to detect relationships between people, vehicles/property, locations, and/or crime characteristics.

N-DEX "connects the dots" between data that is seemingly unrelated. N-DEX supports multi-jurisdictional task forces—enhancing national information sharing, linking regional and state records management systems, and enabling virtual regional information sharing.

N-DEX provides **no-fee access** to national data in **real time**, with **results** returned in a matter of seconds, based upon the user's Internet connection.



How Does N-DEX Benefit Me?

Investigative Use

- Conduct nationwide searches from a single access point
- Search names, IDs, people, phone numbers, tattoos, associates, cars, boats, other property, etc.
- Search by modus operandi
- Receive notifications and collaborate with others on similar investigations

Strategic Use

- Coordinate task forces
- Identify crime trends
- Use geovisualization and mapping features
- Facilitate deconfliction

Tactical Use

- Identify "hotspots" of criminal activity
- Assess threat level of persons or addresses
- Form additional investigative partnerships
- Enhance officer safety

How Does N-DEX Work?

Electronic records are mapped in Extensible Markup Language, based on the National Information Exchange Model and Logical Entity Exchange Specification standards for electronically sharing criminal justice information. The records are then electronically transmitted to N-DEX.

How do I Participate with N-DEX?

Data Submission:

Please contact an N-DEX Liaison Specialist at 304.625.4242 to discuss data submission criteria and capabilities.

User Access:

To access to the N-DEX system, visit the Law Enforcement Online (LEO) Web site, <www.leo.gov>, and scroll to the bottom of the Sign On page. Click on the link to secure an N-DEX SIG membership and follow the steps that are displayed.

What's the Next Step?

Sign up to begin sharing data and begin searching the N-DEX system. Call 304.625.4242 today!

HOW DOES N-DEX BENEFIT ME? -CONTINUED



The N-DEX User Interface

The easy-to-use interface allows users to search all N-DEX data fields from the main search tab on the homepage. To conduct a search with more specific controls, users may click the Advanced Search tab located to the right of the main search tab.

N-DEX features a set of filters along with a Reason and History tab, which are located along the left side of the home page.

The filters may be used on any search and may be applied to the results as well. Filters can be used individually or in combination with one another.

Filters include geographic location, date, data sources, result filters, and external filters. This functionality provides fine granularity for searching and narrowing search results.

State-of-the-art tools for viewing, analyzing and understanding the data returns can be accessed via the tabs at the top of the page. Also, targeted search links reside above the N-DEX logo and provide the user with the option to specifically define a search for people, places, and things.

Key points to Remember

- Participating agencies own and maintain the sharing of their data.
- The N-DEX system includes active and up-to-date case files.
- Sharing controls allow submitters to define exactly how and what kind of data they want to share.
- No fees are required to access N-DEX.
- Data must not be disseminated, nor any law enforcement action taken, without first contacting the record-owning agency.
- Training is available for both N-DEX users and administrators. Computer-based training modules are available at <www.leo.gov>, and hands-on training may be requested by contacting the N-DEX Program Office.

N-DEX Contact Info

N-DEX Information Hotline: 304.625.4242
 For technical problems: 304.625.4357
 Email: <ndex@leo.gov>
 Web site: <http://www.fbi.gov/about-us/cjis/n-dex>
 Jeffrey C. Lindsey, Program Manager 304.625.4219

Send your N-DEX Success Story to the
 Program Office
 Email: <ndex@leo.gov>

U.S. Department of Justice
 Federal Bureau of Investigation
 Criminal Justice Information Services Division



N-DEX

THE RIGHT INFORMATION
 IN THE RIGHT HANDS
 RIGHT NOW



WHAT DO YOU NEED TO KNOW?

AFIS INTERFACE WITH OTHER STATES

ELY MEZA—KBI

As part of Kansas's automated fingerprint identification system (AFIS) contract with MorphoTrak, Inc., an interface with the Missouri State Highway Patrol (MSHP) has been implemented.

Kansas law enforcement agencies have the option to send criminal fingerprint identification searches to the MSHP AFIS, providing that the submitting livescan is using at least Kansas NIST

Map version 5.1 submission standards. This interstate search functionality was built into the submission standard six years ago, and it has been made operational.

The inter-AFIS system allows Kansas to search latent prints against the other state's tenprint databases as well. This functionality is controlled and managed by the Latent Examination Section in

the KBI Laboratory.

When a livescan operator selects the option to search another state AFIS, the record will be forwarded to the selected (currently only MSHP) state(s) thru the KBI AFIS. The manner in which this option is presented to the operator varies by livescan model; each vendor has incorporated this differently.

Continued on Page 17

AFIS INTERFACE WITH OTHER STATES—CONTINUED

This functionality is just an option; **it is not mandatory for any agency to search other state AFIS databases.**

Furthermore, there are a limited number of searches that can be exchanged each day, so this functionality should be used only when there is an operational reason.

The submitting agency will receive AFIS messages from the Central Repository at the KBI without any change to the current process. In addition to the

standard KBI messages, corresponding identification responses from Missouri are sent to the agency's designated e-mail address. Another message will be sent to the agency's primary KCJIS (*Open Fox*) terminal.

The following data elements should be part of the livescan operating system software.

Description= Inter-State Identification

Field Name=Connected States

Code

Tag= 2.711

Tag Name=KIS

Field Number=2004


Field Name=Connected States Code

OFFENDER REGISTRATION Q AND A

JESSICA DULTMEIER - KBI

Q. What date should be used in the *registration date* box on the Kansas Offender Registration Form?

KANSAS OFFENDER REGISTRATION FORM



The form includes the Kansas Bureau of Investigation (KBI) seal and a section for the State's Attorney (SO) to use, with fields for Birth month, 2nd Reg Visit, 3rd Reg Visit, and 4th Reg Visit. Below the seal, it says "PLEASE PRINT OR TYPE ALL INFORMATION". The main form fields are: AGENCY ORI NUMBER, REGISTRATION DATE, KBI NUMBER, FBI NUMBER, and COURT DETERMINED SEXUAL PREDATOR (YES/NO).

A. Enter the date the offender is physically registering with your agency. Having the correct registration date is an important factor in determining an offender's compliance. Tip: The *registration date* box and date on the *signature of registrant* should match.

Q. If an offender is required to register in multiple KS counties, are they required to report the same information to all counties?

A. Yes, it is essential for each registering agency to collect all applicable information on the KS Offender Registration form. It is equally important that offenders report the same information to every agency where they are required to register. For example, on a registration form from Agency A the offender's employment is entered as Spangles with a complete address, however on a registration form from Agency B, no employment information is entered. Tip: Ask the offender if they have a copy of the registration form completed at another agency and compare or use the information on the form being completed by your agency.

ADVANCED AUTHENTICATION REQUIREMENT EXTENDED

Captain Randy D. Moon - Kansas Highway Patrol – CJIS Systems Officer

Currently, the CJIS Security Policy, Section 5.6.2.2.1, Advanced Authentication (AA) Policy and Rationale, states AA is required when accessing Criminal Justice Information (CJI) outside the boundary of physically security location with physical, personnel, and technical security controls implemented. Section 5.6.2.2.1 contains interim compliance designating a police vehicle as a physically secure location to permit authorized users accessing CJI within a police vehicle to be exempt from the AA requirements until September 30, 2013.

Section 5.6.2.2.1 contains additional interim compliance stating IPsec (Internet Protocol Security – Provides secure Internet Protocol communications) may continue to be utilized to meet the AA requirements until 2013 if it was implemented to meet the CJIS Security Policy version 4.5 requirements.

On Wednesday, 2/13/2013, the APB Chair and APB Executive Committee requested the FBI extend Section 5.6.2.2.1 of the CJIS Security Policy's interim compliance for *police vehicles* and *IPsec* to meet the AA requirements for an additional year. The Executive Committee conveyed their concern over the possibility of law enforcement expending fiscal resources to implement a policy requirement that may be subject to change as a result of a topic going to the Working Groups this March. The committee felt that extending the interim compliance dates for a police vehicle to be considered a physically secure location for the purpose of AA and IPsec implemented to meet CJIS Security Policy version 4.5 requirements (Section 5.6.2.2.1) for an additional year will prevent unnecessary expenditures while the topic moves through the process.

The FBI has agreed to the request with the understanding that this topic will be voted upon at the June APB meeting. Effective immediately, compliance for the IPsec extension and extension for police vehicles to be considered physically secure locations for the purpose of AA will both be 9/30/2014.

The following paragraphs reflect the extension to the CJIS Security Policy:

(CJIS Security Policy changes reflected by old language struck through and new in bold italics)

5.6.2.2.1 Advanced Authentication Policy and Rationale

The requirement to use or not use AA is dependent upon the physical, personnel and technical security controls associated with the user location. For example, AA shall not be required for users requesting access to CJI from within the perimeter of a physically secure location (Section 5.9), when the technical security controls have been met (Sections 5.5 and 5.10). Conversely, if the technical security controls have not been met AA shall be required even if the request for CJI originates from within a physically secure location. Section 5.6.2.2.2 provides agencies with a decision tree to help guide AA decisions.

ADVANCED AUTHENTICATION REQUIREMENT EXTENDED

Captain Randy D. Moon - Kansas Highway Patrol – CJIS Systems Officer

INTERIM COMPLIANCE:

1. For interim compliance, users accessing CJI from devices associated with, and located within, a police vehicle are exempt from the AA requirement until September 30th 2013 **2014** if the information system being used has not been procured or upgraded anytime after September 30th, 2005. For the purposes of this policy, a police vehicle is defined as an enclosed criminal justice conveyance with the capability to comply, during operational periods, with Section 5.9.1.3.
2. Internet Protocol Security (IPSec) does not meet the 2011 requirements for advanced authentication; however, agencies that have funded/implemented IPSec in order to meet the AA requirements of CJIS Security Policy v.4.5 may continue to utilize IPSec for AA until 2013 **September 30, 2014**. Examples:
 - a. A police officer runs a query for CJI from his/her laptop mounted in a police vehicle. The police officer leverages a cellular network as the transmission medium; authenticates the device using IPSec key exchange; and tunnels across the cellular network using the IPSec virtual private network (VPN). IPSec was funded and installed in order to meet the AA requirements of CJIS Security Policy version 4.5. AA requirements are waived until 2013 **September 30, 2014**.
 - b. A detective accesses CJI from various locations while investigating a crime scene. The detective uses an agency managed laptop with IPSec installed and leverages a cellular network as the transmission medium. IPSec was funded and installed in order to meet the AA requirements of CJIS Security Policy version 4.5. AA requirements are waived until 2013 **September 30, 2014**.

EXCEPTION:

AA shall be required when the requested service has built AA into its processes and requires a user to provide AA before granting access. EXAMPLES:

- a. A user, irrespective of his/her location, accesses the LEO website. The LEO has AA built into its services and requires AA prior to granting access. AA is required.
- b. A user, irrespective of their location, accesses a State's portal through which access to CJI is facilitated. The State Portal has AA built into its processes and requires AA prior to granting access. AA is required.

ADVANCED AUTHENTICATION REQUIREMENT EXTENDED

Captain Randy D. Moon - Kansas Highway Patrol – CJIS Systems Officer

5.9.1 Physically Secure Location

A physically secure location is a facility or an area, a room, or a group of rooms within a facility with both the physical and personnel security controls sufficient to protect CJI and associated information systems. The physically secure location is subject to criminal justice agency management control; SIB control; FBI CJIS Security addendum; or a combination thereof.

Sections 5.9.1.1 – 5.9.1.9 describe the physical controls required in order to be considered a physically secure location, while section 5.12 describes the minimum personnel security controls required for unescorted access to a physically secure location. Section 5.6.2.2.1 describes the requirements for technical security controls required to access CJI within the perimeter of a physically secure location without AA.

For interim compliance, and for the sole purpose of meeting the advanced authentication policy, a police vehicle shall be considered a physically secure location until September 30th 2013 **2014**. For the purposes of this policy, a police vehicle is defined as an enclosed criminal justice conveyance with the capability to comply, during operational periods, with Section 5.9.1.3.

Although the extension is in place until September 2014 we encourage agencies to continue to work towards meeting the advanced authentication requirement in order to meet the new deadline. If you are unsure if your agency needs to meet AA, please contact Mr. Don Cathey, Information Security Officer, at dcathey@khp.ks.gov or 785-368-6518.

R.A.P.I.D.

REPORT AND POLICE IMPAIRED DRIVERS

JOE MANDALA—KBI

Status Report, 29 April 2013

Most of the first quarter of 2013 was spent working on detailed design for the RAPID project. At the time of writing, the detailed design documents have been completed. Additionally, a fairly significant scope clarification was negotiated, which will result in no-cost change orders during the year's second quarter.

PROJECT ACTIVITY – THROUGH 2013 Q1

The month of January saw the creation of the initial design documents. Initial detailed design review was held on February 5th and 6th. Identification of areas in need of further development, modification, and correction were made, and that work followed throughout the remainder of the quarter.

This phase of the project can seem slow to some, but it is critical to the success of the project. Time and effort spent now can avoid problems later, and while it may not seem like much is happening, this is one of the most involved portions of a project's lifecycle. We would again like to thank those stakeholders who engaged in our active feedback process, and who gave us extremely important information in developing our detailed design.

Continued on Page 21

R.A.P.I.D.**REPORT AND POLICE IMPAIRED DRIVERS—CONTINUED**

The following design documents were developed, reviewed, and approved during this process:

- Audit-Logging
- Court Imaged Documents
- Dissemination Library
- Enterprise Level Design
- Filings and Dispositions
- KCJIS Portal Migration – Static Content
- QA Notification*
- RAPID Global References
- Subscription/Notification
- Unified Search

User Authentication/Authorization

*subsequently de-scoped

While the majority of the quarter was spent in design work, a push to complete the Filings and Dispositions design early in the quarter allowed development work to begin on that most important part of the project. Additionally, other parts of the project started initial development, notably the Dissemination Library (which was essentially completed).

Several demonstrations of the initial mock-ups of the KADR and KJDR submission forms were held (one part of the Filings and Dispositions design), which were received to strongly positive reviews. Feedback from those sessions was incorporated into the final design documentation. Additional demonstrations are planned.

UPCOMING PROJECT ACTIVITY

The coming quarter (2013 Q2) will see work beginning (and in some cases continuing) on development items for Sub-Project 2.2: Core Components – RAPID Portal.

With design for this sub-project largely behind us, we will be focusing on the core of this sub-project.

The test plan should be completed early in the quarter. We will be asking for stakeholder review of the test plan to ensure that it will meet the expectations of the user community. Look for this sometime near the end of June.

Development work that will proceed during second quarter includes:

- DUI Search – Core Components and User Interface
- BOLO (Be On the Lookout) Search Migration and Integration
- Development of the Electronic Court Filings and Dispositions Framework
- Development of Project Plans for Sub-Projects 2.3 - 2.6

Continued on Page 22

R.A.P.I.D REPORT AND POLICE IMPAIRED DRIVERS—CONTINUED

In order to provide an information exchange packet document (IEPD) with which the courts will be able to develop a solution for electronic filing, the framework will need to be completed as early as possible in the project. This is why we have been working so hard on design, and have pushed these items so strongly to the forefront. Since this is a legislative requirement, we hope to get this documentation out the door and into the hands of those who need it by third quarter for testing.

As soon as that is done, we will turn our attention to developing detailed plans for the following sub-projects.

MAJOR MILESTONES

The following milestones were completed in the preceding reporting period:

- Initial design reviews held Feb 5th and 6th
- KADR/KJDR Stakeholder Review Feb 25th
- Scope Clarification completed Apr 1st

DELIVERABLES COMPLETED

This is a list of deliverables completed and milestones reached in the reporting period. The “WBS Task #” column refers to a specific related task in the project plan.

<i>Deliverable Name</i>	<i>WBS Task #</i>	<i>Original Due Date</i>	<i>Adjusted Due Date</i>	<i>Date Delivered</i>

LATE DELIVERABLES AND MILESTONES

There is one late deliverable for the reporting period, though it has subsequently been delivered.

<i>Deliverable Name</i>	<i>WBS Task #</i>	<i>Original Due Date</i>	<i>Adjusted Due Date</i>	<i>Date Delivered</i>
Core Component Design	33	1/30/13	3/4/13	

UPCOMING DELIVERABLES AND MILESTONES

This is a list of deliverables to be completed and expected milestones to reach in the next reporting period.

FROM THE DNA DATABANK**JOHN GAUNTT—KBI**

So far in 2013, the KBI DNA Databank has received almost 4,000 DNA samples, an average of 231 samples a week.

- 3289 arrestees
- 440 convicted offenders
- 224 registered offenders
- 1 court order

Where did they come from, you might ask. Here is the breakdown.

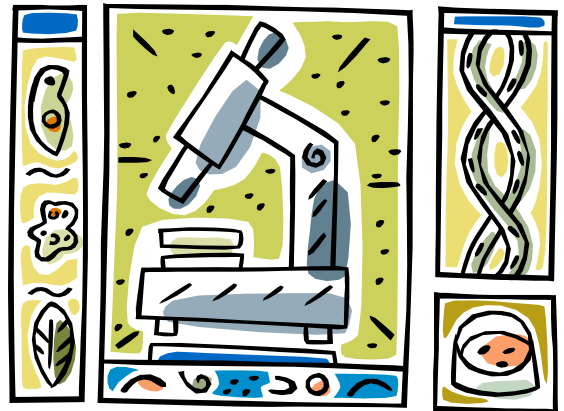
- 90 Sheriff Offices
- 33 Court Service offices
- 30 Community Corrections programs
- 9 Juvenile Detention Centers
- 5 Correctional Facilities
- 4 Police Departments

Through the remainder of this year, we will encourage more agencies to implement the Prelog method of documenting the DNA sample. The Prelog program is linked to a KCJIS record check. The record check informs the user if an offender has already been collected for the Databank. With a couple mouse clicks, the Prelog program opens up to an easy to complete document. The Prelog program comes with up-to-date statutes and a training program.

We benefit also. Our staff is able to process a Prelog sample quicker yet we still perform due diligence on every submission before the sample is processed for importation to CODIS. The more significant benefit to our staff is the lower number of duplicate samples to process. After a year of Prelog, the number of duplicate samples have decreased by 30 percent.

This may seem difficult to imagine, but we have received a fourth DNA sample for some offenders. Remember: DNA collection is a singular event for any qualifying offender. At least two of every three qualifying Kansas offenders have already been collected CODIS.

The Prelog program virtually eliminates duplicates because the link to access Prelog would not appear for offenders already in the Databank. If your agency is considering the Prelog program, please contact me at the KBI Biology Section.



Continued on Page 24

FROM THE DNA DATABANK—CONTINUED

Here is one tidbit of housecleaning while I have you here. If your KCJIS record check response does not reveal a State ID (KBI number), the person does not have criminal history. Unfortunately on rare instances, the DNA Sample on File field may not reveal the DNA flag [Y or N] to give you access to the Prelog program.

The screenshot displays the KCJIS Master Search Results page. The browser address bar shows the URL: https://www.kcjis.state.ks.us/Database_Searches/Master_Search/default.aspx. The page title is "Master Search Results". The navigation bar includes "Home", "Logout", "SEARCH", "INFORMATION", and "WEB SWITCH". The main heading is "Kansas Criminal Justice Information System KCJIS".

The "Summary of Criminal Information" section is divided into three main categories:

- Identifiers:**
 - FBI No. :
 - State ID :
 - Offender Reg. No. :
 - DNA Sample On File :
- Demographic Information:**
 - Sex :
 - Race :
 - Height :
 - Weight :
 - Hair : XXX
 - Eye :
 - Source : [Warrant](#)
- Aliases:**
 - Names : [Redacted] ([Warrant](#)), [Redacted] ([Warrant](#)), [Redacted] ([Warrant](#))
 - Dates of Birth : [Redacted] ([Warrant](#))
 - Social Security Numbers : [Redacted] ([Warrant](#))

The "Mugshot Data:" section on the right indicates "No Photo Available".

One possibility for this occurrence is to look at the "Data Sources" that have been checked on your query. Here are your options:

- Criminal History
- Registered Offender
- BOLO
- Misdemeanor Warrants
- Corrections

FROM THE DNA DATABANK—CONTINUED

If you have them all of these selected and your record check does not give you a KBI number, there is no Kansas criminal history. If the offender qualifies for the DNA Databank and you want to use Prelog, you will need to click on the New Search tab on the lower right area of the screen. Select *only* Criminal History as your Data Source as I have done here.

Database Searches - Kansas Criminal Justice Information System - Microsoft Internet Explorer provided by KBI

https://www.kcjis.state.ks.us/Database_Searches/default.asp?bolJSEnabled=True

File Edit View Favorites Tools Help

Database Searches - Kansas Criminal Justice Informat...

Home | Logout SEARCH INFORMATION WEB SWITCH

Kansas Criminal Justice Information System KCJIS

Search

Mugshot Data: Photo Album

Select a purpose:
Criminal Investigation(KC)

Search Initiated For:
tpkbbjsg

Choose a Search Type
☒ Person Search
☐ Vehicle Search

Data Sources : ☒ Criminal History ☐ Registered Offender ☐ BOLO ☐ Misdemeanor Warrants ☐ Corrections

:: Unique Identifier Search

Select an Identifier

:: Demographic Search

The demographic search is for exact and wildcard matches only.

For example, providing 'SEA*(* being the wildcard) in the last name field will return all candidates with last ...

Last Name: First Name: Middle Name:

This record check result would give you access to the Prelog program.

John Gauntt, Program Consultant for the Biology Section

NEWS FROM THE KBI HELP DESK

WILSON WILEY—KBI

Central Message Switch Updates and Fixes

Over the last few months, the KBI Help Desk has been busy putting in fixes and new features on the message switch that we hope will make your job easier. To start, let's go through a few fixes that we put in:

The attention field on the Kansas KFQ now shows up in the correct place and is populated correctly. Fixed 4/11/2013.

Submitting a BOLO with 6 or more destinations will now work. Fixed 4/10/2013.

Submitting a KCS with the LIS set to a state other than Kansas will now only send an NLETS RQ transaction instead of the RQ and KVQ to KDOR. Fixed 4/10/2013.

OpenFox Desktop hardware fingerprinting fix to stop the invalid/corrupt license files. Implemented 2/20/2013.

OpenFox Desktop Java 7 compatibility fix. Implemented 2/20/2013. The KBI Help Desk has tested and will support Java versions through Java 7 Update 21 as of 4/29/2013.

And here are a few updates that we have implemented:

The Kansas KYQ and KYR hit confirmation message keys should only be used to send hit confirmation messages for Kansas Misdemeanor Warrant records, not for NCIC records. NCIC records should be confirmed using the YQ and YR message keys. Removed the ability to perform hit confirmations for NCIC records through the KYQ and KYR message keys. Implemented 4/10/2013.

The Kansas KAM and BOLO forms (EBOL/MBOL) were updated in OpenFox Messenger to make the destination fields have a drop-down that includes a list of Kansas broadcast groups (similar to the NLETS AM form). Implemented 4/25/2013.

Central Message Switch Tips and Tricks

Here are a few tips and tricks we have found over the last few months that we want to share with everyone:

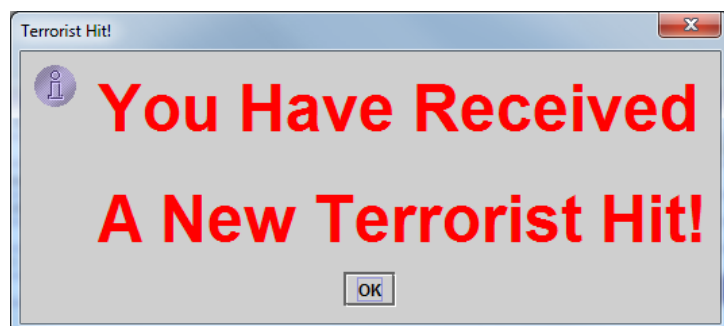
If you're doing an FAA aircraft query using the GQ form, leave off the "N" character that appears at the beginning of the aircraft number found on the tail of the aircraft. Including the "N" in the aircraft number will likely result in a "no record" return.

If you're querying a vehicle, registration, or operator license number (OLN), you will probably want to use the DQ or RQ message keys. NLETS provides two other message keys, the RNQ (Registration Name Query) and the DNQ (Driver Name Query) message keys, however, these two message keys are not supported by very many states. The RNQ message key is supported by ten states while the DNQ message key is only supported by one state. For comparison, all 50 states support and will respond to a DQ or RQ transaction. NLETS provides a service map to see what transactions each state supports. You can view the service map from the NLETS website here: <https://www.nlets.org/service-map>.

NEWS FROM THE KBI HELP DESK—CONTINUED

Terrorist Hits

The KBI recently implemented new functionality on the message switch that allows for greater alert and notification capabilities for terrorist hits in NCIC. When you run a query to NCIC and the return includes a terrorist record, the message switch will automatically copy the transaction to the Kansas Fusion Center to notify them. If you ran the query from an OpenFox Messenger terminal, OpenFox will also activate an alert window that must be acknowledged. The alert window will look like this:



In addition, the messages in your Messenger Inbox with terrorist hits will be displayed with purple text, similar to this:

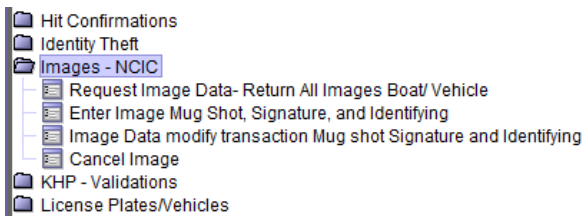
QWKCS	TPKKBWRW	NCIC		Apr 30, 2013 12:25:35	UNKNOWN	✗		
QW	TPKKBWRW	NCIC	QW: NAM=EXAMPLE, CATEGORY THREE DOB=19190101	Apr 30, 2013 12:23:22	2428	✗		
QW	TPKKBWRW	NCIC	QW: NAM=EXAMPLE, CATEGORY THREE DOB=19190101	Apr 30, 2013 12:23:21	2428	✗		
ACK	TPKKBWRW	SWITCH	QW: NAM=EXAMPLE, CATEGORY THREE DOB=19190101	Apr 30, 2013 12:23:21	2428	✓		
QW	TPKKBWRW	NCIC	QW: NAM=EXAMPLE, CATEGORY THREE DOB=19190101	Apr 30, 2013 12:07:25	2427	✗		
QW	TPKKBWRW	NCIC	QW: NAM=EXAMPLE, CATEGORY THREE DOB=19190101	Apr 30, 2013 12:07:25	2427	✗		
ACK	TPKKBWRW	SWITCH	QW: NAM=EXAMPLE, CATEGORY THREE DOB=19190101	Apr 30, 2013 12:07:24	2427	✓		
KCS	TPKKBWRW	ELMERS2	KCS: NAM=EXAMPLE, CATEGORY THREE DOB=19190101 SEX=M	Apr 30, 2013 12:07:10	2426	✓		
QWKCS	TPKKBWRW	NCIC	KCS: NAM=EXAMPLE, CATEGORY THREE DOB=19190101 SEX=M	Apr 30, 2013 12:07:09	2426	✗		
ACK	TPKKBWRW	SWITCH	KCS: NAM=EXAMPLE, CATEGORY THREE DOB=19190101 SEX=M	Apr 30, 2013 12:07:08	2426	✓		
QW	TPKKBWRW	NCIC	QW: NAM=EXAMPLE, CATEGORY THREE DOB=19190101	Apr 30, 2013 11:59:20	2425	✗		
ACK	TPKKBWRW	SWITCH	QW: NAM=EXAMPLE, CATEGORY THREE DOB=19190101	Apr 30, 2013 11:59:20	2425	✓		

To determine if this is an actual hit, compare the details of the terrorist record with what you queried. Many NCIC hits are based solely on a date of birth match, meaning most of the terrorist hits will be “false” hits. However, due diligence must be performed to ensure that an actual hit is not missed. If you discover that the person you queried is the subject of a terrorist record in NCIC, in addition to calling the FBI Terrorist Screening Center, you should immediately follow up with the Kansas Fusion Center as well. Procedures for this new functionality are still being put in place. We will provide the phone number to call for the Kansas Fusion Center at a later date once the procedures are finalized.

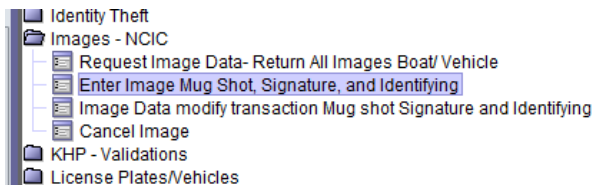
NEWS FROM THE KBI HELP DESK—CONTINUED**Image Support in NCIC**

NCIC has the ability to append images to records. This is a great tool to make sure that another agency will be able to accurately identify the person or property that your agency enters into NCIC. You can follow these steps to append an image to an NCIC record.

1. Enter your person or property record into NCIC (this means you've gotten a response from NCIC with a NIC number).
2. In the OpenFox Messenger Forms Tree, open the 'Images - NCIC' folder.



3. Double-click the link for 'Enter Image Mug Shot, Signature, and Identifying' to open the EIM form.

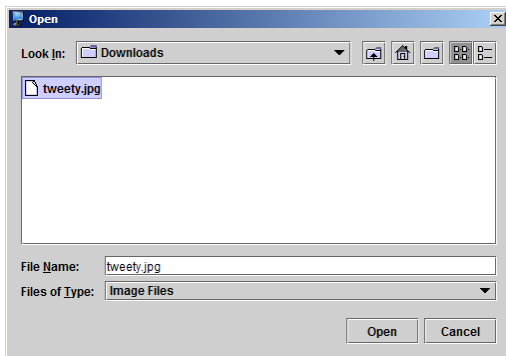


4. Once the EIM form is open, enter the NIC number for the record of the person or property that the image will be appended to. Also select the image type, enter in the date of the image, and any other information into the miscellaneous field. Once all necessary information has been filed out on the form, click the 'Import Image' button.

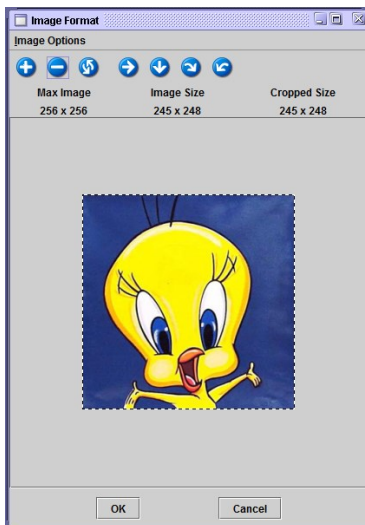
A screenshot of a web-based form titled 'EIM - NCIC Enter Image'. The form is divided into several sections: 'Header Information' with a dropdown for 'ORI' and a 'Control Field' input; 'Required Information' with fields for '* NCIC # (NIC)' (containing 'W240010155'), '* Image Type (IMT)' (a dropdown menu showing 'M = Mugshot'), and 'Date of Image (DOI)' (containing '20130428'); 'Image Data' with 'Import Image' and 'Format Image' buttons and a large red 'X' placeholder; and 'Miscellaneous Information (MIS)' with a text area containing 'THIS IS A TEST IMAGE FOR A TEST RECORD'. At the bottom are 'Submit', 'Clear', and 'Close' buttons.

NEWS FROM THE KBI HELPDESK—CONTINUED

5. In the next window that comes up, locate the image file from the local computer that will be appended to the NCIC record. Select the image file, and click the 'Open' button.



6. The image processing window will come up. In this window, you can modify the image to get it to display correctly. Image adjustments include enlarging or reducing the image size, returning the image to its original size, flipping the image horizontally or vertically, as well as rotating it clockwise or counter-clockwise. Once the image has been corrected, click the 'OK' button.



NEWS FROM THE KBI HELP DESK—CONTINUED

7. You will then be returned to the main EIM form screen and the image will be populated in the Image Data area. All that's left now is to submit the transaction.

8. Once the transaction has been submitted, you will receive a confirmation message from NCIC. NCIC assigns a unique number to each image, called the IMN.

TL0100KZ,MRI5708374

KSKBI0000

IMAGE IS ACCEPTED

NIC/W240010155 IMN/I210060354 IMT/M


Because more agencies are starting to append images to their records in NCIC, it's helpful to query NCIC with the image indicator flag set to Yes. With the image indicator flag set to Yes, the images that are appended to records in NCIC will be returned in line with the rest of the response. For example, using the QW form, fill out the information needed to submit the transaction. At the bottom of the QW form, there are a group of optional fields, one of them being the Image Indicator (IND) field. Select the drop-down for this field and select 'Y = Yes'. You can then submit the QW transaction.

Continued on Page 31

NEWS FROM THE KBI HELP DESK—CONTINUED

The response from NCIC will look like this:

```

TL0100KZ,MRI5709406
KSKBI0000
***MESSAGE KEY QW SEARCHES WANTED PERSON FILE FELONY RECORDS REGARDLESS OF
EXTRADITION AND MISDEMEANOR RECORDS INDICATING POSSIBLE INTERSTATE
EXTRADITION FROM THE INQUIRING AGENCY'S LOCATION. ALL OTHER NCIC PERSONS
FILES ARE SEARCHED WITHOUT LIMITATIONS.
MKE/WANTED PERSON
EXL/1 - FULL EXTRADITION UNLESS OTHERWISE NOTED IN THE MIS FIELD
ORI/KSKBI0000 NAM/TEST,TEST T SEX/M RAC/W
DOB/19850218 HGT/511 WGT/155 EYE/BRD HAI/BLK
OFF/TREASON
DOW/20130428 OCA/TESTOCA-123
HQA/N
DNA/N
ORI IS KS BUR INVESTIGATION TOPEKA 785 296-8262
IMN/I210060354 INT/M
NIC/W240010155 DTE/20130429 0511 EDT DLV/20130429 0511 EDT
IMR/
Begin Image
Image Type: M
NAM:TEST,TEST T DOB:19850218
RAC:W HGT:511 WGT:155 DOI:20130428

NIC:W240010155 IMN:I210060354
MIS:THIS IS A TEST IMAGE FOR A TEST RECORD
End Image

```

In addition to the Query Wanted (QW) form, the Image Indicator field is available in the Query Article (QA), Query Article Batch (QAB), Query Boat (QB), Query Boat Batch (QBB), Query Gang Member (QGM), Query Identity Theft (QID), Query Image (QII), Query Vehicle (QV), Query Vehicle Batch (QVB), Query Protection Order (QPO), Query Sex Offender (QXS), Query Unidentified (QU), Query Wanted Batch (QWB), and Query Wanted/III (QWI) forms.

Criminal History Record Searches

When you're doing searches on the KCJIS Web Portal for a criminal history record, it's important to not be too specific in your search. By being too specific, you may be narrowing down your search too much and excluding records that could be a possible match to what you're searching for. For example, submitting a search with an eye or hair color that's not on the record you're looking for may result in it not hitting on your search. In that case, it would be better to leave those fields blank. To help alleviate this issue, the search page on the KCJIS Web Portal is defaulted to a date of birth range of plus or minus 5 years, a height range of plus or minus 5 inches, and a weight range of plus or minus 20 lbs. We recommend starting off with a broad search criteria and then narrowing down the results with subsequent searches.

Demographic Search

Last Name:	First Name:	Middle Name:
<input type="text"/>	<input type="text"/>	<input type="text"/>
Date of Birth:	Age:	
mm dd yyyy	<input type="text"/> +/- <input type="text"/> Years	
Race:	Sex:	
<input type="text"/>	<input type="text"/>	
Height:	Weight:	
ft in +/- <input type="text"/> in	lbs +/- <input type="text"/> lbs	
Hair Color:	Eye Color:	
<input type="text"/>	<input type="text"/>	

Continued on Page 32

NEWS FROM THE KBI HELP DESK—CONTINUED

Other News

In other news, the Nlets Help File on the KCJIS Web Portal has been replaced with a new manual that is based off of Nlets' Wiki pages. The new manual is available here:

<https://www.kcjis.state.ks.us/Information/nlets/nletstoc.asp>

Windows XP Support Ends Soon

Microsoft has announced that support for Windows XP will end on April 8, 2014. After that time Microsoft will no longer issue security patches and updates. This poses a great security risk to your agency and to the KCJIS network in general if computers are not able to get new security patches to defend against hackers and malware. Your agency should plan to be completely moved to Windows Vista or Windows 7 by 2014 (32 and 64 bit versions are both supported). With the new version of SecuRemote that we just released in February of this year, there's no reason to hold back your migration. We are also requesting that agencies make sure that Internet Explorer is kept updated. All computers used for KCJIS will need to have at least Internet Explorer 8 (and preferably Internet Explorer 9) installed by 2014. For a complete list of the computer specifications that the KBI Help Desk supports, please see the KCJIS Computer Specifications document on the KCJIS Web Portal here:

https://www.kcjis.state.ks.us/information/audit/Minimum_KCJIS_Computer_Specs.pdf



KBI

Molly Bickel
1620 SW Tyler
Topeka, KS 66612

Phone: 785-296-8266
Email: molly.bickel@kbi.state.ks.us

The KCJIS NEWSLETTER is published by the Kansas
Criminal Justice Coordinating Council

Derek Schmidt

Chairman

Attorney General

Sam Brownback

Vice Chair

Governor

Council Members:

Kirk Thompson, Director
Kansas Bureau of Investigation

Justice Nancy Moritz,
Chief Justice Designee

Ray Roberts, Secretary of
The Kansas Department of Corrections

Ernest Garcia, Superintendent of
The Kansas Highway Patrol

Terri Williams, Commissioner
Juvenile Justice Authority

Caleb Stegall,
Governor Designee

Lee Davidson, Attorney
General Designee